

Forum:[Hack Forums](#)

Thread: [UnSlaveMe | Fully undetectable does simply not matter](#)

Forc?d - July 5, 2015, 12:52 pm

[img]http://#/rZLnYf.png[/img]

THIS IS THE PROGRESS THREAD, THE SOFTWARE IS NOT YET FOR SALE.

There is tons of software on HF to encrypt,spread,connect,log,mine etc.
But not really any to "help" or prevent the users of HF to become an slave/being infected.

So this is just that. "UnSlaveMe" is a software designed to undo anything happening to your computer after a certain point.
Removing miners, loggers,rats etc with ease.No need for Sandbox or setting up a virtual machine (As many or most malware has many types of antis that defeats such tools)

Spoiler ([Click to View](#))

You simply launch "UnSlaveMe", click 1 button to generate a "Snapshot" of the current computer state/information and run the suspicious file.

If it turns out to be a malware you are 1 button away from removing it.

This unlike typical Bot-killers and Anti-Viruses does not "detect" anything or use any sort of database.

It basically takes what the user has defined as an white-list (The system at an "clean" state) and compares that to how the system appears afterword, removing the difference. Therefore it does not matte if the file is FUD,UD or heavily detected.

Along the process it also outputs a log that show how the malware deploys and operates, making the application not only helpful for removing but also doing general researching.

UnSlaveMe's destructive power can not only be used to remove malware, with features on the "to do" list like

detecting changes made to the registry. You may easily be able revert the "xx Days trial period" on certain programs.

Spoiler ([Click to View](#))

[img]http://vvcap.net/db/JMwMyM7S3EOO-RYtEPZB.png[/img]

[img]http://vvcap.net/db/LHCa1zHNUXPbNCZW7-yN.png[/img]

[img]http://vvcap.net/db/aKxG0pGuj6gN6i_v52JR.png[/img]

[Video: <https://www.youtube.com/watch?v=0mRPQXnOCYg>]

-To Do List-

*Automatically detect changes made to the registry, act on that information

*Fully Integrate NetSeal

-Changelog per.11.07.2015-

Fixed issue where the software does not re-run the removal process

Re-coded main removal function for better stability and cleaned up some mess

Added new "Settings" menu to easily manage the features

Added an Anti-Persistence feature

Added Custom process termination (for user to define specific process to kill)

Added a "Extreme Mode" feature(basically find the source of any new process executed and kills/removes it. If used wrong can corrupt your system files.)

Added "Disable network" feature

Made if possible for user to define whether or not to kill "explorer.exe" on removal.

Added "Custom ext" makes in possible for users to include or exclude file extensions

Added "Whitelist" so user can define processes or file that are not to be touched.

[img]http://vvcap.net/db/BCx8U1S4jXIZYCTwqk4-.png[/img]

When copy's are available for sale they will ONLY be sold to users of HF. Lifetime license only.

Do you have an advanced malware? Please send me a copy so that i can test it on UnSlaveMe :)

You can also support this project by wearing the official signature! This will also get you a discount coupon code when sales have started.

Code

[url=https://hackforums.net/showthread.php?tid=4894467][align=center][img]https://i.imgur.com/CIHh0RI.gif[/img][[/align]][/url]

LordCoder - July 5, 2015, 12:57 pm

It seems like KL-Detector released back in 2006. But it's quite nice to see a tool like this. How does it detect a silent miner?

Dredd - July 5, 2015, 12:59 pm

Correct me if I'm wrong but the demo there was basically a FileSystem watcher watching the whole system directory just detecting changes?

Forc?d - July 5, 2015, 1:01 pm

(Jul 5, 2015 12:57 PM)LordCoder Wrote: [\[CITE\]](#) It seems like KL-Detector released back in 2006. But it's quite nice to see a tool like this. How does it detect a silent miner?

Like any other file, when you click "Generate snapshots" it collects information about the current system, it also start a logger that logs every .exe moved around your computer.

When you then launch a malware or anything else, i collects and stores information about it. when you click "remove" it compares the old info with the new one. and removes anything that was not on the old system.

It does not "scan" or use any database. Is a matter of detection a "difference" in the system.

(sry my bad english)

(Jul 5, 2015 12:59 PM)? Wrote: [\[CITE\]](#) Correct me if I'm wrong but the demo there was basically a FileSystem watcher watching the whole system directory just detecting changes?

For files being moved yes a file-watcher is being used.

Dredd - July 5, 2015, 1:04 pm

(Jul 5, 2015 01:01 PM)Forc?d Wrote: [\[CITE\]](#) For files being moved yes a file-watcher is being used. FileSystem watcher detects changes to files, new files, deleted files and of course moved files.

Forc?d - July 5, 2015, 1:06 pm

(Jul 5, 2015 01:04 PM)? Wrote: [\[CITE\]](#) FileSystem watcher detects changes to files, new files,

deleted files and of course moved files.
Depends on the filters you set but yes?

Unknown - July 5, 2015, 1:08 pm

Seems quite useful considering there are some sketchy downloads out there (especially in the "Beginner Hacking" section on here). This project definitely has a lot of potential, I'd like to see where it goes!

LordCoder - July 5, 2015, 1:09 pm

(Jul 5, 2015 01:01 PM)Forc?d Wrote: [\[CITE\]](#) Like any other file, when you click "Generate snapshots" it collects information about the current system, it also start a logger that logs every .exe moved around your computer.

When you then launch a malware or anything else, i collects and stores information about it. when you click "remove" it compares the old info with the new one. and removes anything that was not on the old system.

It does not "scan" or use any database. Is a matter of detection a "difference" in the system.

(sry my bad english)

But a silent miner doesn't drop any file to the system, correct? You could add a feature that detects the CPU usage of each process and it's more than 80-85% then remove it.

Forc?d - July 5, 2015, 1:09 pm

(Jul 5, 2015 01:08 PM)PandaNET Wrote: [\[CITE\]](#) Seems quite useful considering there are some sketchy downloads out there (especially in the "Beginner Hacking" section on here). This project definitely has a lot of potential, I'd like to see where it goes!

Thanks for the feedback and interest ?

ze-slade - July 5, 2015, 1:11 pm

I'd definitely be interested in this. Subscribing to thread.

Forc?d - July 5, 2015, 1:12 pm

(Jul 5, 2015 01:09 PM)LordCoder Wrote: [\[CITE\]](#) But a silent miner doesn't drop any file to the system, correct? You could add a feature that detects the CPU usage of each process and it's more than 80-85% then remove it.

Hmmm, that is a nice suggestion. However the programs does end processes that where not active at the time the "snapshot" was taken. But that was a really god suggestion, i may take that somewhere.

Dredd - July 5, 2015, 1:24 pm

(Jul 5, 2015 01:06 PM)Forc?d Wrote: [\[CITE\]](#) Depends on the filters you set but yes?
You said you only use it for files being moved.

Zettabit - July 5, 2015, 1:37 pm

(Jul 5, 2015 01:12 PM)Forc?d Wrote: [\[CITE\]](#) Hmmm, that is a nice suggestion. However the programs does end processes that where not active at the time the "snapshot" was taken. But that was a really god suggestion, i may take that somewhere.

It would be a good idea. What I would do is create a custom structure with options like ProcessName, PID, etc and loop through the current processes into an array. When the user wants to revert, compare the current processes with the previously captured list.

If there are any processes that aren't in the captured list, kill them.

Not a bad idea to be honest. It's nice to see things that are anti-malware instead of malware.

Dredd - July 5, 2015, 1:40 pm

(Jul 5, 2015 01:37 PM)Zettabit Wrote: [\[CITE\]](#) It would be a good idea. What I would do is create a custom structure with options like ProcessName, PID, etc and loop through the current processes into an array. When the user wants to revert, compare the current processes with the previously captured list.

If there are any processes that aren't in the captured list, kill them.

Not a bad idea to be honest. It's nice to see things that are anti-malware instead of malware. He said it already does that look up 2 posts.

Forc?d - July 5, 2015, 1:42 pm

(Jul 5, 2015 01:37 PM)Zettabit Wrote: [\[CITE\]](#) It would be a good idea. What I would do is create a custom structure with options like ProcessName, PID, etc and loop through the current processes into an array. When the user wants to revert, compare the current processes with the previously captured list.

If there are any processes that aren't in the captured list, kill them.

Not a bad idea to be honest. It's nice to see things that are anti-malware instead of malware. That is what it currently does . Thanks! I think so to.

(Jul 5, 2015 01:24 PM)? Wrote: [\[CITE\]](#) You said you only use it for files being moved. ohhhh! Now i see the point. yeah sorry, moved, created, deleted and modified!

Thanks for all the great feedback! Loving the warm welcome of new software here on this forum! :)

Hoody - July 5, 2015, 9:54 pm

Im gonna start by saying nice job bro :)

If i were you i would add memory scanning to it as well :)

heres an example of what you can do

Spoiler [\(Click to View\)](#)

note: the scanner doesnt do anything to the process, just detects it.

Im not gonna give away the source for this cause its used in my botkiller that i DONT want to reFUD. sorry :/

Forc?d - July 5, 2015, 10:13 pm

(Jul 5, 2015 09:54 PM)Hoody Wrote: [\[CITE\]](#) Im gonna start by saying nice job bro :)

If i were you i would add memory scanning to it as well :)

heres an example of what you can do

Spoiler [\(Click to View\)](#)

note: the scanner doesnt do anything to the process, just detects it.

Im not gonna give away the source for this cause its used in my botkiller that i DONT want to reFUD. sorry :/

So this uses the principal of all types of anti-virus right? It scans the memory to find something and it uses something to identify it with? Correct me if I'm wrong. And that the Is not really what I want to achieve here. This program does never need to know what is wrong and wright. No database , nothing. It simply compares what you defined as an clean computer , and kills everything else that was not on that afterwords.

But really cool memory scanner, looks to work great!

debug - July 5, 2015, 10:15 pm

(Jul 5, 2015 10:13 PM)Forc?d Wrote: [\[CITE\]](#) So this uses the principal of all types of anti-virus right? It scans the memory to find something and it uses something to identify it with? Correct me if I'm wrong. And that the Is not really what I want to achieve here. This program does never need to know what is wrong and wright. No database , nothing. It simply compares what you defined as an clean computer , and kills everything else that was not on that afterwords.

But really cool memory scanner, looks to work great!! think both approaches would work well. The memory scanner should work regardless of it being crypted, but then again you do have a point. Your version is pretty sweet because there need not be any predefined values to compare.

Hoody - July 5, 2015, 10:26 pm

(Jul 5, 2015 10:13 PM)Forc?d Wrote: [\[CITE\]](#) So this uses the principal of all types of anti-virus right? It scans the memory to find something and it uses something to identify it with? Correct me if I'm wrong. And that the Is not really what I want to achieve here. This program does never need to know what is wrong and wright. No database , nothing. It simply compares what you defined as an clean computer , and kills everything else that was not on that afterwords.

But really cool memory scanner, looks to work great!

Thats is correct, i guess you could go off of just comparing what files change. It would just be nice to have all the "common" malware in a scanner though, since it seems like your making an antivirus. But i guess if your using this kinda like sandboxie, that isnt helpful to you.

DragonHunter - July 5, 2015, 10:49 pm

This looks pretty nice tbh, the demo already shows it's already working, I'm wondering if you'd even be able to isolate just 1 program.

If you could isolate (like select a program/process) it would be neat, because you wouldn't be running just 1 program, you'd have browsers, skype, games or whatever

My guess aswell is that, if you'd add registry changes, it would be funny to bypass those Time Limit programs, just unslave and registry changes are gone ?

Hoody - July 5, 2015, 11:00 pm

(Jul 5, 2015 10:49 PM)DragonHunter Wrote: [\[CITE\]](#) My guess aswell is that, if you'd add registry changes, it would be funny to bypass those Time Limit programs, just unslave and registry changes are gone ?

That is a genius idea. Where can i purchase?

Forc?d - July 5, 2015, 11:07 pm

(Jul 5, 2015 10:49 PM)DragonHunter Wrote: [\[CITE\]](#) This looks pretty nice tbh, the demo already

shows it's already working, I'm wondering if you'd even be able to isolate just 1 program.

If you could isolate (like select a program/process) it would be neat, because you wouldn't be running just 1 program, you'd have browsers, skype, games or whatever

My guess aswell is that, if you'd add registry changes, it would be funny to bypass those Time Limit programs, just unslave and registry changes are gone ?

What ever programs that runs when the software is launched when not be to touched.

Will demonstrate this in next video. But i have been on the idea of isolating programs. Maybe create an permanent whitelist.

Never really thought about the use for this software in resetting trial periods. But that is an great idea also, any new suggestions on a better name for the software are warmly welcomed.

(Jul 5, 2015 10:49 PM)DragonHunter Wrote: [\[CITE\]](#) This looks pretty nice tbh, the demo already shows it's already working, I'm wondering if you'd even be able to isolate just 1 program.

If you could isolate (like select a program/process) it would be neat, because you wouldn't be running just 1 program, you'd have browsers, skype, games or whatever

My guess aswell is that, if you'd add registry changes, it would be funny to bypass those Time Limit programs, just unslave and registry changes are gone ?

What ever programs that runs when the software is launched when not be to touched.

Will demonstrate this in next video. But i have been on the idea of isolating programs. Maybe create an permanent whitelist.

Never really thought about the use for this software in resetting trial periods. But that is an great idea also, any new suggestions on a better name for the software are warmly welcomed.

(Jul 5, 2015 10:49 PM)DragonHunter Wrote: [\[CITE\]](#) This looks pretty nice tbh, the demo already shows it's already working, I'm wondering if you'd even be able to isolate just 1 program.

If you could isolate (like select a program/process) it would be neat, because you wouldn't be running just 1 program, you'd have browsers, skype, games or whatever

My guess aswell is that, if you'd add registry changes, it would be funny to bypass those Time Limit programs, just unslave and registry changes are gone ?

What ever programs that runs when the software is launched when not be to touched.

Will demonstrate this in next video. But i have been on the idea of isolating programs. Maybe create an permanent whitelist.

Never really thought about the use for this software in resetting trial periods. But that is an great idea also, any new suggestions on a better name for the software are warmly welcomed.

(Jul 5, 2015 11:00 PM)Hoody Wrote: [\[CITE\]](#) That is a genius idea. Where can i purchase?

Will be for sale hopefully when I have sorted out some bugs and added some more features.

Tidas - July 5, 2015, 11:20 pm

Neato. Reminds me of Deep Freeze.

Forc?d - July 6, 2015, 7:47 am

Bump, thread has been updated. Any suggestions are warmly welcomed either here or on PM.

+Haze - July 6, 2015, 7:58 am

I want dat sauce code bruh

Minato Namikaze - July 6, 2015, 8:04 am

Sucks you got to pay for it.

Guess im sticking to Sandboxie :(

apawow - July 6, 2015, 8:38 am

This seems like a very helpful program, I can't wait for you to release it.

krazyk - July 6, 2015, 8:55 am

Wow this looks really cool...I am very interested in this.

XuidDump - July 6, 2015, 9:09 am

That's pretty sweet.

Good program man, definitely looking forward to this.

VmX5 - July 6, 2015, 2:11 pm

I'm quite interested on how you managed to do a "Snapshot" of the system Because on a normal PC (not vm) the drive will not be blank there WILL be other files The program will not be able to take a "snapshot" in a matter of seconds are you just using a FileSystemWatcher?

Also remember if this tool becomes popular people could just make a bypass for your tool (Find if a process(Your program) is open and kill it)

Forc?d - July 6, 2015, 2:17 pm

(Jul 6, 2015 02:11 PM)VirusCrafter5 Wrote: [\[CITE\]](#) I'm quite interested on how you managed to do a "Snapshot" of the system Because on a normal PC (not vm) the drive will not be blank there WILL be other files The program will not be able to take a "snapshot" in a matter of seconds are you just using a FileSystemWatcher?

Also remember if this tool becomes popular people could just make a bypass for your tool (Find if a process(Your program) is open and kill it)

"Snapshot" is in this case a fancy name for the program collection necessary information.

This software is for the HF community (which I hope no one plan to infect) I therefore hope there will be now "anti-unslaveme" but I have plans in place if that may be the case.

VmX5 - July 6, 2015, 2:27 pm

Could you explain how the "Snapshot" works or is that something secret? (Share if you can) please.

Forc?d - July 6, 2015, 2:42 pm

(Jul 6, 2015 02:27 PM)VirusCrafter5 Wrote: [\[CITE\]](#) Could you explain how the "Snapshot" works or is that something secret? (Share if you can) please.

It mainly gathers proses, file information and deloys ressources used for later. Like what processes are running, ID,parent file location. This is all under development and Will get more advanced (if it needs to)

log dot zip - July 6, 2015, 2:54 pm

(Jul 6, 2015 02:42 PM)Forc?d Wrote: [\[CITE\]](#) It mainly gathers proses, file information and deloys ressources used for later. Like what processes are running, ID,parent file location. This is all under development and Will get more advanced (if it needs to)

If you need any help cleaning up some code, or developing further on this idea, please feel free to PM me. If you for whatever reason decide to discontinue development on this, I could see myself rewriting perhaps a more extensive version of this from scratch.

?irito - July 6, 2015, 2:56 pm

This looks like an amazing program.

log dot zip - July 6, 2015, 3:11 pm

I am quite new around here, and this site has quite a few restrictions set in place for newer users (understandably so with all the spam bots going around). So let's talk somewhere else. If you PM me your Skype, or any other (convenient) mean of contacting you, we'll be in touch shortly.

VmX5 - July 6, 2015, 3:19 pm

Cool, Very nice job by the way You could add a few things and I see your project having the potential to be a professional commercial product.

Randy_Savage_xX - July 6, 2015, 8:14 pm

Looks sweet man, can't wait to try it! :D

Forc?d - July 11, 2015, 11:25 am

BUMP, thread has been updated. Who'd also like people to send me any-kind of malware so i can start testing this on other thing then DarkComet, Imonitor,Babylon and AthenaBot

SubGenius - July 11, 2015, 11:55 am

That's a nice piece of work mate... might find it usefull someday.
Muh Thanksz.

Forc?d - July 11, 2015, 3:51 pm

Just updated the thread with a new demo video, showing some more muscles! Please check and maybe some feedback? BUMPx2

hackersallin - July 12, 2015, 1:45 am

If i am able to test it out on my PC and it removes all the viruses my PC currently has and all the problems... I will pay you instantly!! I probably won't pay before hand because i have tried other software.. they didn't remove all... for example, i am even unable to open my Task Manager... so i had to install another software to look at my task manager, for another, my msconfig does not open up. Wtf.

Anyways, cool project, would DEFINITELY buy if it works!

Forc?d - July 12, 2015, 2:13 pm

(Jul 12, 2015 01:45 AM)hackersallin Wrote: [\[CITE\]](#) If i am able to test it out on my PC and it removes all the viruses my PC currently has and all the problems... I will pay you instantly!! I probably won't pay before hand because i have tried other software.. they didn't remove all... for example, i am even unable to open my Task Manager... so i had to install another software to look at my task manager, for another, my msconfig does not open up. Wtf.

Anyways, cool project, would DEFINITELY buy if it works!

Thanks for the feedback, i think at the point of release this software will help you

VmX5 - July 12, 2015, 6:07 pm

How much do you plan to sell it for when you do sell it?

Forc?d - July 13, 2015, 3:16 am

(Jul 12, 2015 06:07 PM)VirusCrafter5 Wrote: [\[CITE\]](#) How much do you plan to sell it for when you do sell it?

I'm thinking 10-15 USD for lifetime, will only sell lifetime

(Jul 12, 2015 06:43 PM)Odinz Wrote: [\[CITE\]](#) Does this work only with known malware? I'm certain I can break it.

It uses a system that works on malware that uses files and process.
Known or not does not matter as it does not try to specifically work with some specific malware.
Send me an stub and I will test to see if it removes it.

Don't really understand what you mean by "break it" , creating antis was a thing I was hoping people whoud avoid doing , as the software is intended for users of the forum only.

Zyklon A - July 14, 2015, 3:00 pm

Can your software detect hooks and system wide injection?

Forc?d - July 15, 2015, 4:08 am

(Jul 14, 2015 03:00 PM)Joca Amsterdam Wrote: [\[CITE\]](#) Can your software detect hooks and system wide injection?

The software operates on a much simpler level, but is still very effective

In depends on how that changes the computer information, I'f there is an change it detects,, it will act on it. Currently it does not collect process size or dumps in memory, so any process running on the snapshot event will not be killed, even if the process size/dump has changed. However any new process started with payload injected (or not) will be killed, it will also try to see what process is handeling/denying access on files.

Currently i am working on the execution steps(what the software will act on first,second etc..) to get best/stable results. I also received an BetaBot build to test with, will give update on that as I may be a better answer to your question.

Hope that answers your question.

prof.dracula - July 15, 2015, 7:07 am

This tool looks good. Thanks for sharing with the community, op.

¹³³⁷ - July 15, 2015, 10:19 pm

Wow very impressive tool keep it up ?

Angel Beats?? - July 15, 2015, 10:24 pm

(Jul 5, 2015 09:54 PM)Hoody Wrote: [\[CITE\]](#) Im gonna start by saying nice job bro :)

If i were you i would add memory scanning to it as well :)

heres an example of what you can do

Spoiler [\(Click to View\)](#)

note: the scanner doesnt do anything to the process, just detects it.

Im not gonna give away the source for this cause its used in my botkiller that i DONT want to reFUD. sorry :/

pretty shitty botkill if all it does is scan memory for known sigs lol

?I??? ??t - July 16, 2015, 10:00 am

how are you going to prevent rootkits ?

Best Regards,

GSOmega

Forc?d - July 16, 2015, 11:28 am

(Jul 16, 2015 10:00 AM)GSOmega Wrote: [\[CITE\]](#) how are you going to prevent rootkits ?

Best Regards,

GSOmega

As of right now i think Rootkits are a bit out the league for this software, i will be optimizing the software for a bit softer types of malware like Rats,Keyloggers,Miners etc.. But i am working on it!

CyberTechnologyInc - July 16, 2015, 6:49 pm

(Jul 5, 2015 12:59 PM)? Wrote: [\[CITE\]](#) Correct me if I'm wrong but the demo there was basically a FileSystem watcher watching the whole system directory just detecting changes?

Why would any sane person buy this? Any experienced programmer could make something like this in a day or two...

Don't get me wrong, it's a cool idea, but it's extremely easy to make.

Forc?d - July 16, 2015, 10:01 pm

(Jul 16, 2015 06:49 PM)CyberTechnologyInc Wrote: [\[CITE\]](#) Why would any sane person buy this? Any experienced programmer could make something like this in a day or two...

Don't get me wrong, it's a cool idea, but it's extremely easy to make.

Why whoud any sane programmer in HF buy any other crypter/logger etc? Are they not as easy to make ?

CyberTechnologyInc - July 17, 2015, 6:23 am

No, they aren't as easy to make as this program is.

Also, what happens when malware starts to add themselves to the white list?

Every new release, it would be pretty easy for people to find out where this white list is stored, then they'd just add themselves to it. Then your system is pretty useless.

Forc?d - July 17, 2015, 6:59 am

(Jul 17, 2015 06:23 AM)CyberTechnologyInc Wrote: [\[CITE\]](#) No, they aren't as easy to make as this program is.

Also, what happens when malware starts to add themselves to the white list?

Every new release, it would be pretty easy for people to find out where this white list is stored, then they'd just add themselves to it. Then your system is pretty useless.

The white-list is not stored in a file on disk, it is stored in memory.

If people think this is so easy to make and it is useless, they will not buy it.

Simple as that, everyone has an Opinion?

How hard is it to make an eBook? Not very hard, however they sell like wildfire with the correct advertising and somewhat handy information.

BahNahNah - July 17, 2015, 7:27 am

(Jul 17, 2015 06:59 AM)Forc?d Wrote: [\[CITE\]](#) The white-list is not stored in a file on disk, it is stored in memory.

If people think this is so easy to make and it is useless, they will not buy it.

Simple as that, everyone has an Opinion?

How hard is it to make an eBook? Not very hard, however they sell like wildfire with the correct advertising and somewhat handy information.

So it doesn't save settings? Even so, memory can be edited. Also, couldn't this be overloaded by

dropping a bunch of files and running them or just continually editing temp files?

Forc?d - July 17, 2015, 9:12 am

(Jul 17, 2015 07:27 AM)BahNahNah Wrote: [\[CITE\]](#) So it doesn't save settings? Even so, memory can be edited. Also, couldn't this be overloaded by dropping a bunch of files and running them or just continually editing temp files?

Really if you start to think that way, there is much simpler ways to "defeat" this application.

However that should not be the intention behind this.

This software is mainly aimed for those ho tests and spreads malware, not the guy ho gets infected. Like a side tool to test your own application on yourself to check crypter compatible etc.. Of-course it can be used the other way around, as an precaution, but not the main aim.

That is why this is only on HF and is relatively simple.

Also the reason i was hoping to not have to deal with a bunch of functions made specifically to defeat this software.

CyberTechnologyInc - July 18, 2015, 12:22 pm

If this program is aimed specifically at people that test and spread malware, and not the guy that gets infected, why are you even bothering to make this program? I'm pretty sure that people that know how to make malware are able to remove their own. And one of it's purposes is to test their malware? Anti-viruses such as malware-bytes are more likely a better option for them to use, you'd probably be better off releasing this open-source, allowing beginners to learn from it.

Visual Freedom - September 20, 2015, 6:37 am

@Forc?d Keep your work up, it will help people!

taktaktak - September 20, 2015, 8:08 am

couldn't you just use sandboxie?

Illusionisten - September 20, 2015, 3:22 pm

Run trough the process list and add processes with 50%+ usage to a suspicious list